PHDE 030217 EPP

IB/2004/050841

Europäisches Patentamt | European Patent Office | Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

03101778.3 ✓

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 03101778.3
Demande no:

Anmeldetag:
Date of filing: 18.06.03
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Diebstahlsicherungssystem für mobile elektronische Geräte

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04M1/667

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

BESCHREIBUNG

Diebstahlsicherungssystem für mobile elektronische Geräte

Die Erfindung betrifft ein mobiles Gerät, ein Diebstahlsicherungssystem sowie ein Verfahren zur Diebstahlsicherung eines mobilen Gerätes.

Mobile Geräte mit einem Mobilteil und einer Basisstation sind bekannt. Derartige Geräte sind als tragbare oder mobile Einheiten bezüglich ihrer Größe und ihres Gewichts optimiert, damit diese leicht transportiert werden können. Diese Eigenschaften ermöglichen jedoch eine erleichterte Entwendung durch unberechtigte Personen, wenn die Geräte lediglich für Sekunden unbeaufsichtigt bleiben.

Heutige Mobilteile sind mittels Diebstahlsicherungssystemen gegen eine Benutzung durch unberechtigte Personen gesichert. Als Beispiel sei hier z.B. die Verwendung von SIM-Karten in Mobiltelefonen genannt. Ein Hauptnachteil bei der Sicherung mittels SIM-Karte ist darin zu sehen, dass die Mobiletelefone weiter verwendet werden können, wenn die SIM-Karte ausgetauscht wird.

Weiter lassen sich andere mobile Geräte, wie zum Beispiel Organizer usw. mittels eines Passwortes schützen, so dass Speicher in dem Organizer gegen einen Zugriff einer unberechtigten Person geschützt sind. Nachteiligerweise lassen sich die Organizer nach der Durchführung einer kompletten Löschung dennoch benutzen, wobei allerdings vorher gespeicherte Daten gelöscht sind.

In der GB 2 320 397 A ist ein Mobiltelefon mit einem Diebstahlsicherungssystem offenbart. Hierbei wird der Gebrauch des Mobiltelefons unterbunden, wenn das Mobiltelefon von der Basisstation entfernt wird. Die Nähe des Mobiltelefons wird mittels eines Sensors überwacht. Der Sensor überwacht auch die Ladespannung aus dem Ladegerät. Der Sensor kann aber auch die Spannung des Akkus bei dessen Aufladung überwachen.

Sobald der Sensor die Spannung nicht mehr erfassen kann, oder sobald die Spannung unter einen bestimmten Schwellenwert fällt, wird das Mobiltelefon unbrauchbar oder ist nur für eingehende Telefonanrufe freigeschaltet. Dasselbe tritt ein, wenn die Spannung für eine vorbestimmte Zeitspanne nicht messbar ist, oder die Spannung für eine vorbestimmte Zeitspanne unter einen bestimmten Schwellenwert fällt.

Der Hauptnachteil ist dabei darin zu sehen, dass stets ein Sicherheitscode über eine Tastatur in das Mobiltelefon eingegeben werden muss, wenn dieses von der Basisstation entfernt wird. Weiterhin ist nachteilig, dass das Mobiltelefon bei Austausch, z.B. des Akkus benutzbar bleibt, und das Diebstahlsicherungssystem so umgangen werden kann.

Der Erfindung liegt die Aufgabe zugrunde ein mobiles Gerät mit einem verbesserten Diebstahlsicherungssystem zur Verfügung zu stellen, das in einfacher Weise aber effizient eine Benutzung des mobilen Gerätes durch unberechtigte Personen ausschließt.

Erfindungsgemäß wird dies erreicht durch ein mobiles Gerät nach Anspruch 1, ein Diebstahlsicherungssystem nach Anspruch 4 und eine Verfahren zur Diebstahlsicherung gemäß Anspruch 10. Abhängige Ansprüche beziehen sich auf bevorzugte Ausführungsformen der Erfindung.

Durch die erfindungsgemäße Ausgestaltung des mobilen Gerätes wird ein Diebstahlsicherungssystem zur Verfügung gestellt, das eine unberechtigte Benutzung des mobilen Gerätes ausschließt.

Die unberechtigte Benutzung wird dadurch ausgeschlossen, dass das mobile Gerät eine Authentifizierungseinheit aufweist, die den Ladestand des Versorgungselements überwacht. Wenn der Ladestand des Versorgungselements erhöht wird, verlangt die Authentifizierungseinheit die Eingabe eines Authentifizierungssignals. Wird kein oder nicht das richtige Authentifizierungssignal erkannt, schränkt die Authentifizierungseinheit den Betrieb der Funktionseinheit bis zur Eingabe eines Authentifizierungssignals ein oder unterbindet den Betrieb völlig.

Da die mobilen Geräte beim Betrieb elektrische Energie aus dem Versorgungselement entnehmen und so der Ladestand stets abnimmt, kann ein entwendetes Gerät nur noch für eine begrenzte Zeit verwendet werden. Jedes Aufladen des Versorgungselement aktiviert die Sperrung, da es einem unberechtigten Benutzer nicht möglich ist, das Authentifizierungssignal bereitzustellen.

Außer einer Erhöhung des Ladestandes kann auch eine sprunghafte Änderung dazu führen, dass ein Authentifizierungssignal überprüft wird. Ein solcher Sprung kann festgestellt werden bspw. wenn bei einem Vergleich des Ladezustandes gegenüber der letzten Überprüfung festgestellt wird, dass die Differenz eine festgelegte Schwelle überschreitet. Bei einem solchen Sprung muss von einem Wechsel des Versorgungselements ausgegangen werden.

Das erfindungsgemäße Diebstahlsicherungssystem sieht zusätzlich zu dem mobilen Gerät eine Basisstation vor. Die Basisstation weist eine zweite Authentifizierungseinheit auf. Diese Einheit erzeugt das benötigte Authentifizierungssignal, das über einen Datenpfad zum mobilen Gerät geleitet wird. Für den Benutzer ist dies besonders vorteilhaft, da er nicht selbst für das benötigte Authentifizierungssignal Sorge tragen muss. Bevorzugt weist die Basisstation auch ein Ladegerät auf, wobei das Authentifizierungssignal mit der Ladespannung übertragen werden kann.

Mobile Geräte im Sinne der Erfindung sind z.B. tragbare mobile Geräte, die vorzugsweise eine mobile Stromversorgung aufweisen. Dies können z.B. Geräte zum Speichern und zur Wiedergabe von Daten, und/oder zur Aufnahme und zum Abspielen von Audio- und/oder Videosignalen sein. Aber auch Kommunikationsgeräte können derartige Geräte sein. Derartige Geräte werden von dem Diebstahlsicherungssystem effektiv geschützt.

Nachfolgend wird eine Ausführungsform der Erfindung anhand einer Zeichnung näher beschrieben. Hierbei zeigt

Fig. 1 eine Prinzipdarstellung eines Diebstahlsicherungssystems.

Wie Figur 1 zeigt, weist ein Diebstahlsicherungssystem 10 ein Mobilteil 12 und eine Basisstation 14 auf.

In dem Mobilteil 12 ist eine bekannte Funktionseinheit 16 angeordnet. Die Funktionseinheit 16 steht hier stellvertretend für die eigentliche Funktion eines mobilen Geräts und umfasst dessen bekannte Einheiten, bspw. eines Organizers (Anzeige, Tastatur und/oder Touchscreen, Speicher, Prozessor usw.), einer Digitalkamera (Bildsensor, Anzeige, Speicher, Prozessor usw.), eines Audio-Players (Laufwerk, Anzeige, Tastatur usw.), eines Mobiltelefons (Anzeige, Tastatur, Mikrophon, Lautsprecher, Sende-/Empfangseinheit, Speicher, Prozessor usw.), oder eines weiteren mobilen, elektronischen Geräts.

Zur elektrischen Energieversorgung des Mobilteils 12 weist dieses ein Versorgungselement 20 auf. Das Versorgungselement 20 ist vorzugsweise eine wiederaufladbare Batterie, i.e. ein sogenannter Akku 20.

In dem mobilen Gerät 12 ist eine Authentifizierungseinheit 22 angeordnet. Die Basisstation 14 umfasst eine weitere Authentifizierungseinheit 23. Die Authentifizierungseinheiten bilden ein Authentifizierungssystem 21. Es sei darauf hingewiesen, dass die in Fig. 1 dargestellten Einheiten von Mobilteil und Basisstation funktionale Einheiten sind, d.h. dass diese Einheiten nicht zwangsläufig auch als separate Baugruppen, z.B. separate elektrische Schaltungen in den Geräten vorhanden sind. Vielmehr können diese Einheiten je nach Anwendung auch gemeinsam mit anderen realisiert sein, so dass bspw. die Authentifizierungseinheit 22 des Mobilteils und Teile der Funktionseinheit 16 als Programm-Module realisiert sein können, die auf einer gemeinsamen CPU ablaufen.

Das Authentifizierungssystem 21 umfasst in dem dargestellten Ausführungsbeispiel zwei Authentifizierungs-Speicherelemente 18a, 18b, wobei das Authentifizierungs-

Speicherelement 18a der Authentifizierungseinheit 22 des Mobilteils und das Authentifizierungs-Speicherelement der Authentifizierungseinheit 23 der Basisstation zugeordnet ist. Die Authentifizierungseinheit 22 verfügt zudem über ein Ladestands-Speicherelement 40.

Die Authentifizierungseinheit 22 ist mit der Funktionseinheit 16 elektrisch verbunden. Die Verbindung ist mittels des Pfeils 24 angedeutet. Weiter ist die Authentifizierungseinheit 22 in dem in Figur 1 dargestellten Ausführungsbeispiel mit dem Akku 20 über einen Datenpfad 26 verbunden, über den ein Signal mit dem aktuellen Ladestand an die Authentifizierungseinheit 22 gegeben wird. Entsprechende Schaltungen zur Ermittlung des Ladezustands eines Akkus sind bekannt.

Die Basisstation 14 ist stationär. Sie dient zur Lagerung des Mobilteils 12 und zum Aufladen des Akkus 20. Hierfür weist sie ein aus dem Netz gespeistes Ladegerät 28 auf. Über geeignete Kontakte, bspw. Steckkontakte, ist das Mobilteil 12 mit der Basisstation 14 verbunden, so dass eine Ladespannung angelegt werden kann. Ein Strompfad 34 führt von dem Batterieladegerät 28 über die Authentifizierungseinheiten 22, 23 zum Akku 20. In einer alternativen Ausführung einer Basisstation handelt es sich um ein mobiles Ladegerät, typischerweise als Steckernetzteil aufgebaut.

Parallel zum Strompfad 34 verläuft in Fig. 1 ein Datenpfad 30. Dieser ist bevorzugt so realisiert, dass die Ladespannung (Gleichspannung) einen aufmodulierten Wechselanteil aufweist, so dass Signale zwischen den Authentifizierungseinheiten 22, 23 ausgetauscht werden können.

Eine alternative Ausführung des Datenpfades 30 verwendet den akustischen Signalpfad zwischen einem im Mobilteil vorhandenen Mikrofon sowie einem in der Basisstation vorhandenen akustischen Signalgeber (Lautsprecher). Insbesondere für Mobiltelefone, deren Mikrofon typischerweise in der Nähe der Ladekontakte angebracht ist, ergibt sich so bei geeigneter Plazierung des akustischen Signalgebers in der Basisstation ein sehr

kurzer akustischer Signalweg. Wählt man die mechanische Anordnung der Basisstation passend, indem z.B. der untere Teil eines Mobiltelefons mit dem Mikrofon in einem Ladeschacht verschwindet, ist die akustische Signalübertragung optisch und akustisch vor Beobachtern geschützt. Darüber hinaus könnte man natürlich für den Menschen unhörbare Ultraschall- oder Infraschallsignale verwenden. Während des Ladevorgangs gibt die Basisstation eine vordefinierte, für die jeweilige Kombination aus Mobilteil und Basisstation eindeutige akustische Signalfolge, z.B. eine Tonfolge, ab.

Eine weitere alternative Ausführungsform des Datenpfades 30 besteht in der elektromagnetischen Kopplung eines kurzreichweitigen drahtlosen Senders in der Basisstation mit einem kurzreichweitigen drahtlosen Empfänger in der Mobilstation. Während des Ladevorgangs werden über diese elektromagnetische Kopplung Signale ausgetauscht.

In den Speicherelementen 18a, 18b ist jeweils ein Authentifizierungsmerkmal (Schlüssel) gespeichert, wobei die Authentifizierungsmerkmale einander zugeordnet sind.

Durch die erfindungsgemäße Ausgestaltung des mobilen Gerätes mit dem Authentifizierungssystem 21 mit den beiden Speicherelementen 18a, 18b wird ein Diebstahlsicherungssystem 10 zur Verfügung gestellt, das eine unberechtigte Benutzung des Mobilteils 12 ausschließt.

Die unberechtigte Benutzung wird dadurch ausgeschlossen, dass die Authentifizierungseinheit 22 den Ladestand des Versorgungselements 20 überwacht. Die Überwachung erfolgt kontinuierlich oder in festgelegten zeitlichen Abständen. Bei jeder Überwachung wird der aktuell ermittelte Ladestand mit dem zuvor ermittelten, im Ladestands-Speicherelement 40 abgelegten Stand verglichen.

Ergibt dieser Vergleich, dass der Ladestand gegenüber der letzten Überwachung gleich oder geringer ist, dann wird das Ladestands-Speicherelement 40 entsprechend aktualisiert. Der Betrieb der Funktionseinheit 16 bleibt dann unberührt.

Ergibt aber der Vergleich, dass der Ladestand gegenüber der letzten Überwachung gestiegen ist (bspw. weil der Akku 20 gegen einen aufgeladenen Akku ausgetauscht wurde oder weil aktuell über den Strompfad 34 der Akku 20 geladen wird), dann verlangt die Authentifizierungseinheit 22 ein Authentifizierungssignal. Alternativ kann das Authentifizierungssignal auch dann verlangt werden, wenn eine Ladespannung angelegt wird.

In der Basisstation 14 enthält der Authentifizerungs-Speicher 18b einen Schlüssel, der dem Inhalt des Authentifizerungs-Speichers 18a zugeordnet ist. Die Schlüssel können bspw. übereinstimmen oder durch eine mathematische Operation einander zugeordnet sein. Von der Authentifizierungseinheit 23 der Basisstation 14 wird ein Authentifizierungssignal anhand des Inhalts des Authentifizierungs-Speichers 18b erstellt und über den Datenpfad 30 gesendet. Wenn der Datenpfad 30 unidirektional ausgebildet ist, kann dies fortlaufend erfolgen, so dass bspw. auf der Ladespannung stets das Authentifizierungssignal aufmoduliert wird. Wenn der Datenpfad 30 bidirektional ausgebildet ist, kann die Authentifizierungseinheit 22 des Mobilteils 12 auch eine Anforderung über den Datenpfad 30 senden, auf die die Authentifizierungseinheit 23 dann mit dem Authentifizierungssignal antwortet.

Im dargestellten Beispiel wird dieses Authentifizierungssignal über den Datenpfad 30 zusammen mit der Ladespannung übermittelt, wie durch symbolisch dargestellte Pulse angedeutet ist. Ebenso können die oben beschriebenen alternativen Ausführungen zur Realisierung des Datenpfades 30 zur Übermittlung des Authentifizierungssignals verwendet werden. Das von der Authentifizierungseinheit 23 ausgesendete Authentifizierungssignal wird auf Übereinstimmung mit dem Inhalt des Speicherelements 18a überprüft. Diese Übereinstimmung kann darin bestehen, dass der Inhalt des Authentifizierungssignals mit dem gespeicherten Inhalt des Speicherelements 18a identisch ist. Die Überprüfung kann jedoch auch umfassen, dass das Authentifizierungssignals durch eine mathematische Operation mit dem gespeicherten Inhalt des Speicherelements 18a verknüpft und anhand des Ergebnisses eine Übereinstimmung festgestellt wird, wie es beispielsweise von asymmetrischen Verschlüsselungs-/Authentifikationsverfahren bekannt ist.

Ergibt die Prüfung des Authentifizierungssignals in der Authentifizierungseinheit 22 eine Übereinstimmung, so erfolgt der weitere Betrieb des Mobilteils 12 und ggfs. der Ladevorgang des Akkus 20 weiter ungehindert.

Ergibt die Überprüfung aber, dass keine Übereinstimmung besteht (z.B. auch weil überhaupt kein Authentifizierungssignal empfangen wurde), dann aktiviert die Authentifizierungseinheit 22 einen Sicherungsmodus des Mobilteils 12 weil anzunehmen ist, dass das Mobilteil unberechtigt benutzt wird.

Für den Betrieb des Mobilteils 12 im Sicherungsmodus gibt es mehrere Möglichkeiten. Einerseits kann ein Strompfad von dem Akku 20 zur Funktionseinheit 16 unterbrochen werden, so dass kein weiterer Betrieb möglich ist. Eine andere Möglichkeit besteht darin, über die Verbindung 24 ein Signal an die Funktionseinheit 16 zu senden, so dass diese ihren Betrieb unterbricht und den Benutzer auf die fehlende Authentifikation hinweist. Schließlich ist es auch möglich, dass die Funktionseinheit 16 in einen eingeschränkten Betriebsmodus versetzt wird, in dem nur Notfunktionen (z.B. Notrufe) möglich sind oder bspw. bei einem Mobiltelefon nur eingehende Anrufe möglich sind, oder bei einer Digitalkamera nur noch die Ausgabe von Photos, nicht aber neue Aufnahmen möglich sind. Zusätzlich ist es möglich, dass die Authentifizierungseinheit 22 den Strompfad 34 unterbricht und so das weitere Aufladen des Akkus 20 unterbindet. Die oben genannten Maßnahmen können geeignet kombiniert werden.

Der Sicherungsmodus wird bspw. erreicht, wenn das Mobilteil 12 dem berechtigten Benutzer entwendet wird, und die Authentifizierungseinheit 22 kein Authentifizierungssignal auf dem Datenpfad 30 erkennt, weil versucht wird, den Akku 20 des Mobilteils 12 direkt an einem herkömmlichen Ladegerät aufzuladen.

Durch diese Maßnahmen ist sichergestellt, dass das Mobilteil 12 für eine unberechtigte Person unbrauchbar ist. Es kann vorgesehen sein, dass die Authentifizierungseinheit 22 den Ladestand des Akkus 20 zusätzlich auf das Unterschreiten einer festen Mindest-

schwelle überwacht und dann ebenfalls eine Authentifikation verlangt. So kann die Zeit, für die ein unberechtigter Benutzer das Gerät nach der Entwendung benutzen kann, begrenzt werden. Je nach dem gewünschten Grad an Datensicherheit ist es durch die vollständige Abschaltung der Funktionseinheit 16 oder den eingeschränkten Betrieb auch möglich sicherzustellen, dass in dem Mobilteil 12 gespeicherte Daten einer unberechtigten Person nicht offenbart werden.

Das Ladestands-Speicherelement 40 ist zweckmäßigerweise als nichtflüchtiger Speicher ausgelegt, so dass der Betrag des gespeicherten Ladestandes des Versorgungselementes 20 auch nach dem Ausschalten des Mobilteils 12 noch zur Verfügung steht, und auch dann, wenn der Akku 20 für eine unbestimmte Zeit aus dem Mobilteil 12 entfernt oder ausgewechselt wurde. Auch die Speicherelemente 18a, 18b sind als nicht flüchtige Speicher ausgelegt.

Selbstverständlich ist es im Sinne der Erfindung möglich, mehrere Mobilteile mittels einer gemeinsamen Basisstation benutzbar zu halten. Erforderlich ist hierzu lediglich, dass in dem jeweiligen Speicherelement der Mobilteile ein zum Authentifizierungssignal des Speicherelementes der Basisstation identisches bzw. zugeordnetes Authentifizierungssignal gespeichert ist.

Vorzugsweise werden die jeweiligen Authentifizierungsmerkmale während der Industrieinstallation bei der Herstellung und Zuordnung der einzelnen Systembausteine zueinander als gemeinsamer Schlüssel in die jeweiligen Speicherelemente 18a, 18b eingegeben. Damit besitzen die Speicherelemente 18a, 18b ein gemeinsames Geheimnis.

Alternativ kann das Speicherelement 18b ein bei der Industrieinstallation eingegebenes, willkürliches Authentifizierungsmerkmal aufweisen. Hierbei wird bei der ersten Benutzung des Mobilteils 12 bzw. bei der ersten Aufladung des Akkus 20 ein Authentifizierungssignal festgelegt und in dem Speicher 18a abgespeichert, d. h. es erfolgt eine Zuordnung. So verfügen Mobilteil 12 und Basisstation 14 über ein gemeinsames Geheimnis und es ist sichergestellt, dass kein anderes Ladegerät mit dem Mobilteil verwendet werden kann.

Selbstverständlich liegt es auch im Sinne der Erfindung, wenn die jeweiligen Authentifizierungsmerkmale von dem berechtigten Benutzer eingegeben bzw. geändert werden.

In einer Weiterbildung kann das Speicherelement 18b eine Vielzahl von Authentifizierungssignalen speichern, so dass eine Vielzahl von Mobilteilen mit der Basisstation 14 betrieben werden können. Günstig ist hierbei, dass ein Datenaustausch mittels der Verbindung 30 in beiden Richtungen zwischen den Authentifizierungseinheiten 22, 23 stattfindet. Das Speicherelement 22 sendet dabei sein Authentifizierungssignal zum Speicherelement 23, welches das übereinstimmende Authentifizierungssignal verifiziert.

Zweckmäßig im Sinne der Erfindung kann die Basisstation auch ein einfaches Ladegerät mit einem Klinkenstecker oder dergleichen sein. Hierbei wäre die Authentifizierungseinheit 23 direkt in dem Ladegerät angeordnet.

In einer erweiterten Ausführung (nicht dargestellt) kann der Akku 20 ebenfalls ein nicht dargestelltes Speicherelement aufweisen. In diesem Speicherelement ist ein Authentifizierungssignal gespeichert, das mit dem Authentifizierungssignal in dem Speicherelement 18a übereinstimmt. Vorzugsweise sind die Authentifizierungssignale in den jeweiligen Speicherelementen 18a, 18b und das des Speicherelementes in dem Akku 20 identisch. Wird nun ein neuer Akku 20 in das Mobilteil 12 eingesetzt, fordert die Authentifizierungseinheit das Authentifizierungssignal aus dem neuen Akku an, weil der gespeicherte Ladestand des ausgetauschten Akkus geringer ist als der Ladestand des Neuen, oder, allgemeiner, der Ladezustand des neuen Akkus vom gespeicherten Stand des alten Akkus abweicht. Stimmen die Authentifizierungssignale nicht überein bzw. sind nicht zugeordnet, so aktiviert die Authentifizierungseinheit 22 den Sicherungsmodus.

Insbesondere auf Reisen wird das Mobilteil 12 häufig für längere Zeit von der Basisstation 14 getrennt sein. Dies erfordert oft den Einsatz von Ersatz-Akkus, wenn keine Möglichkeit zum Aufladen besteht. Günstig im Sinne der Erfindung ist daher, wenn der

jeweilige Akku ein zum Authentifizierungssignal des Speicherelementes 18a passendes Authentifizierungssignal aufweist. Damit lässt sich vorteilhaft das Mobilteil 12 mit allen mit dem passenden Authentifizierungssignal versehenen Akkus benutzen.

Damit bei dieser alternativen Ausführung keine Möglichkeit zur Umgehung des Diebstahlschutzes besteht, weisen die hierbei verwendeten Akkus ihrerseits eine Authentifizierungseinheit entsprechend der oben beschriebenen Einheit 22 auf, die sicherstellt, dass der Akku nur unter Zuführung des passenden Authentifizierungssignals geladen werden kann.

PATENTANSPRÜCHE

1. Mobiles Gerät mit

- einem aufladbaren Versorgungselement (20) zur Versorgung des mobilen Gerätes (12) mit elektrischer Energie,
- Mitteln zur Ermittlung eines Ladestandes des Versorgungselementes (20),
- mindestens einer Funktionseinheit (16);
- und einer ersten Authentifizierungseinheit (22) zur Auswertung des Ladestandes, wobei die Authentifizierungseinheit (22) bei einer Erhöhung und/oder einer sprunghaften Änderung des Ladestandes ein Authentifizierungssignal überprüft, und bei fehlendem oder falschem Authentifizierungssignal den Betrieb der Funktionseinheit (16) zumindest einschränkt.

2. Mobiles Gerät nach Anspruch 1, bei dem

- die Authentifizierungseinheit (22) mindestens ein erstes Authentifizierungs-Speicherelement (18a) zum Speichern eines Authentifizierungsmerkmals aufweist,
- wobei die Authentifizierungseinheit (22) mittels des Authentifizierungsmerkmals das Authentifizierungssignal überprüft, und im Fall einer Übereinstimmung den Betrieb der Funktionseinheit (16) freigibt.

3. Mobiles Gerät nach einem der vorangehenden Ansprüche, bei dem

- in einem Ladestand-Speicherelement (40) ein Betrag des Ladestandes des Versorgungselementes (20) speicherbar ist,
- wobei das Ladestand-Speicherelement (40) bevorzugt ein nicht flüchtiger Speicher ist.

4. Diebstahlsicherungssystem mit

- einem mobilen Gerät (12) nach einem der vorangehenden Ansprüche,
- und einer Basisstation (14),
- wobei die Basisstation (14) eine zweite Authentifizierungseinheit (23) aufweist,
- und die Authentifizierungseinheiten (22,23) über einen Datenpfad (30) derart verbindbar sind, dass Authentifizierungssignale mindestens von der zweiten Authentifizierungseinheit (23) zur ersten Authentifizierungseinheit (22) leitbar sind.

5. System nach Anspruch 4, bei dem

- ein elektrischer Versorgungspfad (34) von der Basisstation (14) zum Mobilteil (12) zum Aufladen des Versorgungselements (20) vorhanden ist.

6. System nach Anspruch 5, bei dem

- der Datenpfad (30) und der Versorgungspfad (34) mindestens teilweise gemeinsame elektrische Leitungen aufweisen,
- wobei bevorzugt der Versorgungspfad (34) mindestens eine Versorgungsspannung aufweist, und Daten auf dem Datenpfad (30) durch eine Modulation der Versorgungsspannung übertragen werden.

7. System nach Anspruch 4 oder 5, bei dem

- der Datenpfad (30) in Form von akustischen und/oder elektromagnetischen drahtlosen Sende- und Empfangseinheiten realisiert ist.

8. System nach einem der Ansprüche 4 bis 7, bei dem

- ein bidirektionaler Datenpfad (30) zwischen der Basisstation (14) und dem Mobilteil (12) besteht.

9. System nach einem der Ansprüche 4 bis 8, mit

- mehreren mobilen Geräten (12)
- und einer Basisstation (14),
- wobei in einem Speicherelement (18b) der Basisstation (14) jeweils Authentifikationsmerkmale für die mobilen Geräte (12) gespeichert sind.

10. Verfahren zur Diebstahlsicherung eines mobilen Gerätes, bei dem

- der Ladestand eines aufladbaren Versorgungselements (20) ermittelt wird,
- und bei einer Erhöhung und/oder einer sprunghaften Änderung des Ladestandes der Betrieb einer Funktionseinheit (16) bis zur Eingabe eines Authentifizierungssignals zumindest eingeschränkt wird.

ZUSAMMENFASSUNG

Diebstahlsicherungssystem für mobile elektronische Geräte

Dargestellt ist ein mobiles Gerät (12) mit einem aufladbaren Versorgungselement (20) zur Versorgung des mobilen Gerätes mit elektrischer Energie. Das mobile Gerät (12) weist Mittel zu Ermittlung eines Ladestandes des Versorgungselementes (20) und mindestens eine Funktionseinheit (16) auf. Weiter weist das mobile Gerät eine Authentifizierungseinheit (22) zur Auswertung des Ladestandes auf, wobei die Authentifizierungseinheit (22) bei einer Erhöhung und/oder sprunghaften Änderung des Ladestandes den Betrieb der Funktionseinheit (16) bis zur Eingabe eines Authentifizierungssignals zumindest einschränkt. Weiter ist ein Diebstahlsicherungssystem (10) beschrieben mit dem mobilen Gerät (12) und einer Basisstation (14) mit einer zweiten Authentifizierungseinheit (23), wobei über einen Datenpfad (38) Authentifizierungssignale mindestens von der zweiten Authentifizierungseinheit (23) zur ersten Authentifizierungseinheit (22) leitbar sind.

Fig. 1

Fig. 1